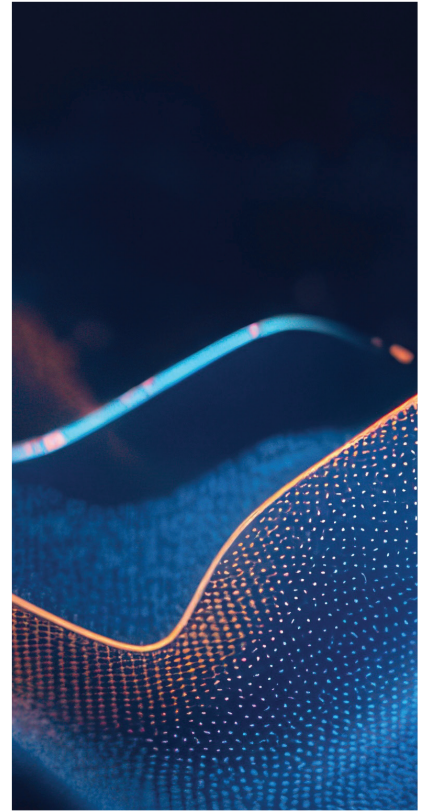
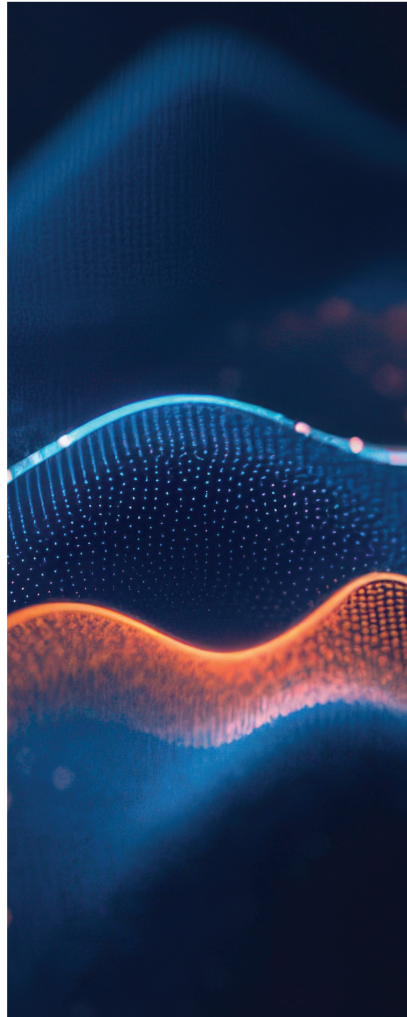


FROST & SULLIVAN
BEST PRACTICES



2026

GLOBAL APPLICATION

DETECTION AND RESPONSE

COMPANY OF THE YEAR



The Transformation of the ADR Industry

The application security industry has expanded rapidly as organizations adopt cloud-native development, microservices, containers, Kubernetes, serverless functions, open-source software, and AI-generated applications.

Traditional appsec testing tools such as static application security testing (SAST), dynamic application security testing, software composition analysis (SCA), and application security posture management (ASPM) remain important for identifying vulnerabilities during development. However, they operate mainly through code analysis, testing snapshots, and aggregated risk scoring, and cannot determine whether a vulnerable function is loaded, executed, and exploitable in a production environment. This leaves security and development teams to face more challenges in managing large theoretical backlogs while attackers increasingly exploit critical vulnerabilities at runtime.

While infrastructure tools like cloud-native application protection platforms (CNAPPs), cloud workload protection platforms (CWPP), endpoint detection and response (EDR), and cloud detection and response (CDR) have strengthened infrastructure and workload visibility, they lack real-time visibility into production applications. They detect suspicious processes, system calls, network connections, container activity, or cloud control-plane events, often after exploitation has already succeeded.

Application runtime security tools (e.g., web application firewalls) add another defensive layer, but operate primarily at the network edge and can be bypassed through novel payloads, internal service paths, compromised dependencies, or attacks that do not resemble known signatures. Runtime application self-protection (RASP) provides deeper application insight. Still, traditional implementations often require intrusive instrumentation, code changes, application restarts, extensive tuning, and developer involvement, limiting scalability across distributed production estates.

These gaps are accelerating demand for application detection and response (ADR), which gives security teams continuous visibility into how applications and their software components behave while running in production. ADR allows organizations to correlate vulnerable code, executed functions, application behavior, and malicious activity, helping them distinguish theoretical exposure from active exploitation. ADR is also evolving beyond application-only monitoring toward cloud application detection and response, connecting the initial application-layer intrusion with subsequent workload, host, Kubernetes, cloud, and AI activity. Frost & Sullivan notes that this broader operating model is increasingly important as security operations centers need a complete attack story across the cloud stack - not another isolated alert stream.

Organization expectations have consequently shifted from finding more vulnerabilities to proving which risks matter, detecting exploitation earlier, and stopping attacks without interrupting production. Organizations still consolidate posture and hygiene controls into broader platforms, but they continue to invest in purpose-built runtime capabilities where those platforms lack code-execution visibility. Frost & Sullivan recognizes how vendors that can cleverly combine precise application insight, low-friction deployment, high-fidelity detection, targeted prevention, and measurable customer outcomes are setting the proper direction of the ADR market.

Addresses Unmet Needs with Disruptive Technology

Founded in 2022, Israel-based Oligo Security has emerged as the leading technology disruptor in ADR by addressing the application-runtime blind spot that remains unresolved by traditional AppSec, CNAPP, CWPP, and other infrastructure-focused detection tools. Its core differentiation is Deep Application Inspection, a non-intrusive runtime capability that observes libraries, functions, call paths, and application behavior while correlating them with operating-system activity. Rather than inferring risk from package presence, static reachability, or configuration data, Oligo identifies what code is actually loaded and which vulnerable functions execute in production. This gives application security teams deterministic context and evidence of exploitability, helping them change vulnerability management from broad prioritization based on probability to focused remediation based on real runtime behavior and context.

Compared to traditional AppSec competitors that provide SCA and ASPM solutions, Frost & Sullivan appreciates the way that Oligo's approach is significantly different. While tools like SCA and ASPM help improve prioritization by generating and aggregating known vulnerabilities and ranking them by severity, asset context, or heuristic reachability, they can still leave teams with thousands of findings that require manual validation. Oligo provides execution-level proof, allowing them to eliminate large volumes of non-relevant risk without narrowing or weakening security coverage. Its real-time bill of materials and Vulnerability Exploitability eXchange context remain aligned with production behavior, giving AppSec and CloudSec teams a granular view of which components are present, loaded, and executed in the runtime

"Compared to traditional AppSec competitors that provide SCA and ASPM solutions, Oligo's approach is significantly different. While tools like SCA and ASPM help improve prioritization by generating and aggregating known vulnerabilities and ranking them by severity, asset context, or heuristic reachability, they can still leave teams with thousands of findings that require manual validation. Oligo provides execution-level proof, allowing them to eliminate large volumes of non-relevant risk without narrowing or weakening security coverage. Its real-time bill of materials and Vulnerability Exploitability eXchange context remain aligned with production behavior, giving AppSec and CloudSec teams a granular view of which components are present, loaded, and executed in the runtime environment. In practice, Oligo customers have been able to reduce vulnerability findings by 70% to more than 99%."

– Anh Tien Vu
Industry Principal, Global Cybersecurity Practice

environment. In practice, Oligo customers have been able to reduce vulnerability findings by 70% to more than 99%.

Oligo also helps teams avoid the deployment and performance limitations that are historically associated with RASP solutions. Its lightweight extended Berkeley Packet Filter (eBPF)-based sensor operates with approximately 1.5% of Central Processing Unit overhead and can be deployed across containers, virtual machines, bare-metal systems, Kubernetes environments, and hybrid infrastructure without requiring source-code access or extensive application instrumentation. The platform supports first-party and third-party applications and provides deep language coverage across Java, .NET, Python, Go, Ruby, and Node.js. This allows Oligo to protect software that organizations build, buy, or use. In contrast, code-scanning products generally lose visibility into these applications and infrastructure packages for which customers do not control the source code.

Oligo also stands out among ADR players through the depth and breadth of the runtime evidence it provides. Some ADR platforms are built on application instrumentation inherited from RASP, giving them strong visibility into application requests and data flows but requiring language-specific agents and deeper integration with application runtimes. Others use distributed tracing, attack-path analysis, or behavioral profiling to map application interactions and determine whether services may be exposed to exploitation. Some cloud-native runtime security competitors often combine ADR with CDR and CWPP. However, their detection is centered more heavily on workload telemetry, application programming interface activity, cloud logs, and infrastructure behavior.

Oligo differentiates itself by directly observing executed libraries, functions, call paths, and their related operating-system actions through a non-intrusive architecture. This allows the platform to determine suspicious activity, the related application component that initiated it, and whether a vulnerable function was executed at runtime. This runtime context can also be extended across first-party applications, third-party software, workloads, cloud infrastructure, and AI components. This combination of deterministic exploitability analysis, code-to-system correlation, broad deployment coverage, and precise runtime prevention gives Oligo a more differentiated position than ADR products focused primarily on application tracing, traditional in-app instrumentation, or infrastructure-level behavioral detection.

By combining application-level depth with broad environmental coverage, Oligo establishes a stronger technical foundation than competitors that provide only network, workload, or syscall telemetry. While many runtime vendors can show that a process started or a system call occurred, Oligo can connect that activity to the specific function and library inside the application that triggered it. This additional layer of context enables more accurate vulnerability prioritization, faster root-cause analysis, and detection of application-originating attacks that remain invisible to tools observing only the surrounding workload.

Delivers Exceptional Customer Value and SOC-Ready Operations

Oligo's ability to produce measurable customer outcomes quickly and with limited operational burden reinforces its technology leadership. The company's solution is deployable within hours or days without requiring code changes or application restarts. Its eBPF-based architecture keeps performance overhead minimal. After deployment, the platform requires minimal ongoing management with only around four hours per week. This makes Oligo attractive to enterprises seeking deeper runtime protection without slowing applications, adding constant tuning requirements, or creating the need for a dedicated specialist team.

Oligo's value extends well beyond technical visibility by delivering measurable improvements in vulnerability management and operational efficiency. Customers reported they have reduced open-source findings and vulnerability backlogs by 70% to more than 99%, while also cutting vulnerability noise by over 80% in some environments. These reductions allow security and development teams to focus on the small number of issues that represent real production risk, rather than spending time validating large volumes of theoretical findings. Oligo also helps automate remediation workflows and provides clear runtime evidence that teams can use during audits, customer assurance reviews, and zero-day response activities. This creates a stronger operational advantage than solutions that improve prioritization but still leave customers with substantial manual investigation.

The platform also helps bridge the operating divide between AppSec, CloudSec, development, and the security operations center (SOC). Oligo provides high-fidelity incident data—including call stacks, process trees, vulnerable-function evidence, and MITRE ATT&CK context—and integrates with security information and event management platforms; extended detection and response platforms; security orchestration, automation, and response platforms; ticketing systems; and developer workflows. This shared runtime evidence enables security, development, and operations teams to investigate and remediate the same verified risks more efficiently. SOC analysts can investigate application attacks without relying entirely on developers to reconstruct execution paths, while developers receive a smaller and more credible set of remediation tasks. Oligo’s 24x7 support and guided onboarding further strengthen operationalization, covering sensor deployment, integrations, response workflows, and cross-team adoption.

This customer-centric model compares favorably with large platform vendors that provide broad coverage but require heavier administration, as well as emerging runtime vendors whose technical depth has not yet translated into repeatable enterprise outcomes. Oligo combines fast deployment, low overhead, precise detection, and targeted blocking with direct evidence of reduced workload. Customers are not buying another source of alerts; they are replacing uncertainty and manual triage with runtime proof.

Converts Technology Leadership into Exceptional Global Growth

Oligo has successfully translated its differentiated runtime security technology into exceptional commercial growth. Frost & Sullivan estimates that the company grew approximately 200% year over year (YoY) in 2024 and became the largest ADR vendor by revenue, an impressive achievement for a company that emerged from stealth only in 2023. Oligo continued this strong momentum in 2025, recording explosive growth (estimated 300% YoY) and strengthening its position as the largest and one of the fastest-growing vendors in the ADR market.

“Oligo has successfully translated its differentiated runtime security technology into exceptional commercial growth. Frost & Sullivan estimates that the company grew approximately 200% year over year (YoY) in 2024 and became the largest ADR vendor by revenue, an impressive achievement for a company that emerged from stealth only in 2023. Oligo continued this strong momentum in 2025, recording explosive growth (estimated 300% YoY) and strengthening its position as the largest and one of the fastest-growing vendors in the ADR market.”

– Anh Tien Vu
Industry Principal, Global Cybersecurity Practice

The company’s customer base includes Fortune 500 organizations and enterprises across banking and financial services, technology, retail and eCommerce, media and entertainment, healthcare, and other application-intensive industries. Most of these customers are cloud-first organizations in North America and Europe that operate complex, distributed applications and need deeper visibility into runtime risk. This customer profile aligns closely with Oligo’s strengths in detecting application-layer attacks, identifying genuinely exploitable vulnerabilities in production, and reducing large vulnerability backlogs.

Oligo’s growth is also driven by its first-mover advantage in addressing gaps left by traditional CNAPP, SAST, SCA,

and cloud detection tools. These solutions provide valuable posture, code, and infrastructure visibility but often lack insight into running code, active library usage, function execution, and real exploitability. Oligo addresses this blind spot by providing runtime visibility inside applications while connecting that insight with workload and cloud context. This allows the company to complement existing cloud and application security platforms rather than requiring customers to replace their entire security architecture.

The platform's ability to reduce vulnerability noise and improve risk prioritization further strengthens its commercial value. By helping security and development teams focus on vulnerabilities that are active and exploitable in production, Oligo supports faster remediation, better developer productivity, lower operational costs, and stronger return on security investment. This extends its value beyond threat detection and response and makes the platform relevant to AppSec, CloudSec, DevOps, and SOC teams.

This has led to greater investor confidence. Oligo raised \$50 million in Series B funding in January 2025, and \$60 million in August 2026, bringing its total funding to \$140 million. The company has been using this investment to expand product development and global go-to-market operations across North America, Europe, Asia-Pacific, and Japan. It has also strengthened its executive leadership, expanded relationships with value-added resellers, and begun developing partnerships with managed security service providers and managed detection & response providers to broaden customer reach.

Oligo is also expanding its market access through technology integrations, cloud marketplaces, and regulated-market initiatives. Its participation in AWS programs improves purchasing and deployment access. In June 2026, Oligo joined Palantir's FedStart program to accelerate its path toward FedRAMP High and US Department of Defense Impact Level 5 compliance, opening opportunities in highly regulated federal environments.

Focusing on Leadership

Oligo has continued to extend its technology beyond ADR visibility and anomaly detection into full-stack cloud-native application detection and response (CNADR). In 2025, the company expanded Oligo Incidents to correlate application-layer exploitation with workload, host, Kubernetes, and cloud activity, giving SOC and AppSec teams a complete attack story from initial intrusion through post-exploitation. Traditional CDR, CWPP, and EDR products often identify the symptoms of compromise, such as an unusual child process, reverse shell, resource spike, or suspicious network connection. Oligo identifies the application code path that initiated the behavior, links it to subsequent activity, and provides call stacks, process trees, and affected assets for investigation. This moves response closer to the point of entry and reduces the manual correlation required across multiple tools.

The introduction of Runtime Exploit Blocking in April 2026 further strengthens this differentiation. Rather than terminating an entire process, killing a container, or taking an application offline, Oligo detects malicious exploit sequences and blocks the underlying system action at the point of execution while allowing the application to continue operating. Its technique-based approach focuses on reusable exploitation behavior rather than individual payload signatures, enabling a single protection rule to address broad vulnerability classes, including previously unknown attacks. This is a significant

improvement over conventional prevention controls that force security teams to choose between active enforcement and production availability.

Oligo is also extending ADR into software supply chain and AI runtime security. Its CNADR engine combines malicious-package intelligence with per-library behavioral profiling to identify compromised or weaponized dependencies when they execute, closing the gap left by continuous integration/continuous delivery (CI/CD) scanning after software reaches production. In November 2025, Oligo introduced Runtime AI Security, including AI Security Posture Management (AI-SPM) and AI Detection and Response (AI-DR), to discover models, agents, SDKs, and external AI services, maintain a continuously updated AI bill of materials, monitor production behavior, and identify threats such as unsafe model usage, prompt injection, data exposure, and agent abuse. AI-SPM addresses the immediate visibility and governance requirements of most organizations, while AI-DR extends real-time detection and protection to enterprises with more mature AI deployments. This expansion remains coherent with Oligo's core ADR architecture rather than representing a collection of disconnected modules. Deep Application Inspection provides the common runtime source of truth across applications, cloud workloads, software dependencies, and AI systems. Competitors that expanded through separate posture, workload, and detection products often require customers to reconcile multiple data models and consoles. Oligo's approach correlates these layers around actual execution, allowing the platform to preserve its application-level precision while broadening into a more complete runtime security offering.

Oligo's evolution from an ADR specialist into a converged CNADR provider further supports its growth outlook. As organizations increasingly seek unified runtime protection across applications, workloads, cloud infrastructure, and AI systems, Oligo is well positioned to benefit from the shift away from posture-only security toward runtime validation, exploitability analysis, and active detection and response. Large platform vendors have broader distribution but generally lack Oligo's function-level application visibility and precise exploit prevention. Meanwhile, smaller runtime security competitors have not demonstrated the same combination of revenue leadership, enterprise adoption, funding strength, customer impact, and global expansion. This gives Oligo the technology foundation and commercial capacity to sustain its market leadership as ADR and CNADR adoption accelerates.

Conclusion

Oligo has advanced the ADR market from application-runtime visibility toward precise, full-stack detection and active prevention. Its Deep Application Inspection technology provides deterministic insight into executed libraries, vulnerable functions, call paths, and application behavior, allowing organizations to identify real exploitability, detect attacks at their point of origin, and block malicious actions without disrupting production. Frost & Sullivan recognizes how Oligo has also successfully translated its technological strengths into business performance, with its revenue growing explosively year after year, an expanded customer base across the Fortune 500, and expansion toward regulated federal markets in the US and globally.

With its strong overall performance, Oligo earns the 2026 Frost & Sullivan Global Company of the Year Recognition.